UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,760	12/13/2000	Kazuo Watanabe	SONY-U0200	6661

26263 7590 03/21/2008

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
03/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte KAZUO WATANABE

Appeal 2007-3971
Application 09/735,760
Technology Center 2100

Decided: March 21, 2008

Before JEAN R. HOMERE, JAY P. LUCAS, and
ST. JOHN COURTENAY III, *Administrative Patent Judges*.

COURTENAY, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-4, 7-10, 13, and 14. We have jurisdiction under 35 U.S.C. § 6(b).

We Reverse.

THE INVENTION

Appellant's disclosed invention is directed to a method of managing software that prevents illegal use of computer programs by only enabling use of the programs by appropriate users (Spec. 1).

Independent claim 1 is illustrative:

1. A method of managing software use by a software provider for distribution to a user, comprising the steps of:

storing inside the software predetermined first information;

providing the software to a software user on an information storage means prepared corresponding to the software and to be connected to an apparatus for running the software, which information storage means is capable of being accessed by the apparatus in a connected state;

encoding second information by using a first key of a key pair of an open key encoding format; and

transmitting the encoded second information to said software user for said software user to decode said transmitted encoded second information by using a second key of said key pair of said open key encoding format, and to read said first information from said information storage means, and to match said read first information against said decoded second information,

wherein said software is enabled when the information match, and

> wherein the encoded second information is transmitted to the software user for matching the read first information against the decoded second information each time the software user uses said software.

THE REFERENCES

The Examiner relies upon the following references as evidence in support of the rejection:

Uchenick	US 4,458,315	Jul. 3, 1984
Olsen	US 5,758,069	May 26, 1998
Coley	US 5,790,664	Aug. 4, 1998

THE REJECTION

Claims 1-4, 7-10, 13, and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Olsen in view of Uchenick and Coley.

Claims 5, 6, 11, and 12 have been cancelled (App. Br. 14-15).

PRINCIPLES OF LAW

"What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under *§ 103*." *KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1742 (2007). Appellant has the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d

1350, 1355 (Fed. Cir. 1998)). Therefore, we look to Appellant's Briefs to show error in the Examiner's proffered prima facie case. "After evidence or argument is submitted by the applicant in response, patentability is determined on the totality of the record, by a preponderance of evidence with due consideration to persuasiveness of argument." *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

Independent Claims 1, 7, 13, and 14

We consider the Examiner's rejection of independent claims 1, 7, 13, and 14 as being unpatentable over Olsen, Uchenick, and Coley.

Although Appellant has argued additional limitations in the Brief, we conclude that we need only reach the single issue set forth below to decide this appeal.

ISSUE

We decide the question of whether the cited combination of Olsen, Uchenick, and Coley teaches and/or suggests the language of each independent claim that requires "match[ing] said read first information against said decoded second information" where the "second information" is encoded using a first key and decoded using a second key (*see* independent claim 1 and the equivalent language recited within independent claims 7, 13, and 14).[1]

[1] We note that independent claims 13 and 14 adopt an alternative nomenclature by referring to the information that is encoded and decoded as "third information."

ANALYSIS

For convenience, the reasoning of the Examiner with respect to the aforementioned limitations is reproduced below:

> Appellant argues Olsen fails to disclose matching a first information to a second information, which is encrypted using a first key and decrypted with a second key.
>
> With respect to this argument Olsen teaches the use of a RSA pubic key digital signature (see column 10 lines 24-26), when using a digital signature the information is encrypted and included with said information when it is sent. On the receiving end the digital signature is decrypted and compared with the sent information for, among other things, verifying non-repudiation. Therefore, Olsen teaches matching a first information to a second information, which is encrypted using a first key and decrypted with a second key because the public key digital signature algorithm uses two different keys for encryption and decryption.

(Ans. 7).

We reproduce the pertinent portion of Olsen below, with lines 24-26 (relied on by the Examiner) emphasized in italics:

> In addition, the required entries suitably include security information, such as encrypted authentication information. An application may be licensed with no security attributes at all. Alternatively, security attributes may be stored in data field 308, and different attributes may be provided to generate different levels of security. For example, the vendor may use the common certificate security format, which utilizes certain "secrets" incorporated into the license acquisition API to prevent unauthorized modification of the license certificate. The license acquisition API's secretes comprise a set of

> encrypted information, such as the license information plus an activation key, which are provided by a client to gain access to an application. *As added protection, a standard RSA public/private key digital signature may be offered for higher end security. In addition, an attribute may be added which requires the presence of a particular hardware security device, often referred to as a "dongle", to activate the application. Information relating to such security attributes may be included in data field 308.*

(Olsen, col. 10, ll. 12-30).

We begin our analysis by noting that the stated purpose of using "license information plus an activation key" by Olsen's client license acquisition API is to "prevent unauthorized modification of the license certificate" (col. 10, ll. 20-24). In particular, we note that Olsen expressly teaches that the license certificates are stored on the server (*see* Olsen, col. 3, ll. 54-59, i.e., "license certificate database 112"; *see also* "LIC CERT DB 112" as shown in Fig. 1).

We further note that Olsen does not provide any details explaining exactly how a "standard RSA public/private key digital signature" would be implemented to provide "higher end security." (col. 10, ll. 25-26). After reviewing the Olsen reference, we find it unclear whether the public key would be held by the server or the client.

One possibility (if the server holds the public key) is that the RSA standard public/private key digital signature could be used by the server to verify both the authenticity of the client and also the content integrity of the client's license information and/or license key. By preventing unauthorized access to the server's license certificates, it follows that unauthorized modification of the server's license certificates would be prevented.

An alternate possibility, (if the client holds the public key), is that the RSA standard public/private key digital signature could be used to verify the both the authenticity of Olsen's server and also the content integrity of the license certificates stored within the server's license certificate database 112 (Fig. 1). While this would ensure that Olsen's client has accessed an authentic license certificate on the server, it is unclear how this would accomplish Olsen's stated purpose of preventing unauthorized modification of the license certificate located on the server (col. 10, ll. 20-21).

In accordance with the RSA standard, both of the above possibilities would involve using a public key to decrypt an encrypted digital signature that was encrypted using a private key. The decrypted digital signature is then compared (i.e., "matched") against a calculated message authentication code derived from the content of the transmitted message. If there is a match, then the receiver of the message has assurance that the message was unaltered during transmission.

The Examiner states that "[o]n the receiving end the digital signature is decrypted and compared [i.e., matched] with the sent information for, among other things, verifying non-repudiation." (*see* Ans. 7). Thus, the Examiner appears to be corresponding Olsen's "sent information" (i.e., the

client's "license information plus an activation key," col. 10, ll. 22-23) with the claimed "first information" that is matched against the decoded RSA digital signature (corresponding to the decoded second information for claims 1 and 7 and corresponding to the decoded third information for claims 13 and 14).

While the Examiner has relied upon the secondary Uchenick reference to teach and/or suggest storing the claimed "first information" inside the software, we find such application does not comport with matching a decoded digital signature against *a calculated message authentication code derived from the content* of the transmitted message, in accordance with the RSA standard taught by Olsen at column 10, line 25.[2] Clearly the decoded RSA digital signature cannot be matched directly against the content itself (i.e., the decoded RSA digital signature cannot be matched directly against the client's license information plus an activation key purportedly corresponding to the claimed "first information").

After considering the totality of the record before us, it is our view that the weight of the evidence supports Appellant's contention that the Examiner has not sufficiently shown the correspondence between the claim elements and the relevant portions of the cited references to establish a prima facie case of obviousness. For us to affirm the Examiner on this record would require speculation on our part. In particular, we find the gap in the combined teachings of the cited references to be uncomfortably wide and such gap cannot be bridged with theories or speculation. In the

[2] The content or "first information" we consider here is Olsen's client license information plus an activation key, col. 10, ll. 22-23.

alternative, if the Examiner is relying upon an inherent teaching in the cited references, our reviewing court has established that "[i]nherency … may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999).

Therefore, it is our view that the Examiner has not clearly established how the cited combination of Olsen, Uchenick, and Coley teaches "match[ing] said read first information against said decoded second information" where the second information is encrypted using a first key and decrypted using a second key (*see* independent claim 1 and the equivalent language recited within independent claims 7, 13, and 14). *See also* Note 1 above.

Because we conclude Appellant has met the burden of showing error in the Examiner's prima facie case of obviousness by a preponderance of evidence, we reverse the Examiner's rejection of independent claims 1, 7, 13, and 14 as being unpatentable over Olsen, Uchenick, and Coley. Likewise, we reverse the Examiner's rejection of dependent claims 2-4 and 8-10, which depend from independent claims 1 and 7, respectively.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude Appellant has met the burden of showing that the Examiner erred in rejecting claims 1-4, 7-10, 13, and 14 under 35 U.S.C. § 103(a) for obviousness.

DECISION

We reverse the Examiner's decision rejecting claims 1-4, 7-10, 13, and 14.

REVERSED

pgc

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO IL 60606-1080